Revista de Direito, Governança e Novas Tecnologias
Double Blind Review pelo SEER/OJS
Recebido em: 06.07.2016
Aprovado em: 17.12.2016

CIBERSEGURANÇA NA UNIÃO EUROPEIA E NO MERCOSUL: BIG DATA E SURVEILLANCE VERSUS PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET.

CYBERSECURITY IN EUROPEAN UNION AND IN MERCOSUR: BIG DATA AND SURVEILLANCE VERSUS PRIVACY AND DATA PROTECTION ON THE INTERNET.

[1]Rafaela Bolson Dalla Favera
[2]Rosane Leal da Silva

RESUMO

Este artigo objetiva discutir as práticas de *surveillance*, com o auxílio do *big data*, especialmente após as revelações de Edward Snowden em 2013. Visa analisar a atuação da União Europeia quanto à *cibersegurança*, além de expor e discutir as eventuais estratégias existentes no Mercosul para enfrentar esses problemas, o que culminará com a análise do Marco Civil da *Internet* no Brasil. Constatou-se a necessidade de os integrantes de um mesmo bloco atuarem de forma transnacional e cooperativa, tal como preconizam as Diretivas da União Europeia, apostando-se em estratégias de segurança *cibernética* colaborativas, em prol dos direitos humanos e fundamentais.

Palavras-chave: *Cibersegurança*; Mercosul; Privacidade; *Surveillance*; União Europeia.

ABSTRACT

This paper aims to discuss the surveillance practices, with the help of big data, especially after the revelations of Edward Snowden in 2013. It aims to analyze the acting of European Union in relation to the cybersecurity, besides to expose and discuss any existing strategies in Mercosur to face these problems, which will culminate with the analysis of the Internet Civil Mark in Brazil. It was found the need for the same block members act of transnational and cooperative manner, as recommended by the European Union Policies, betting on collaborative cybersecurity strategies, in favor of human and fundamental rights.

Keywords: Cybersecurity; Mercosur; Privacy; Surveillance; European Union.

[1] Mestranda do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria – UFSM, Rio Grande do Sul, (Brasil). Linha de Pesquisa: Direitos na Sociedade em Rede e Integrante do Núcleo de Direito Informacional da Instituição. E-mail: rafaeladallafavera@hotmail.com
[2] Doutora em Direito pela da Universidade Federal de Santa Maria – UFSC. Professora do Curso de Graduação e Mestrado em Direito da Universidade Federal de Santa Maria. Coordena o Núcleo de Direito Informacional (UFSM).

INTRODUÇÃO

Recentemente, no ano de 2013, Edward Snowden revelou o maior esquema de espionagem e vigilância *cibernética* da história do governo norte-americano. As violações do direito à privacidade e dados pessoais foram tão intensas que afetaram pessoas físicas e jurídicas, bem como Estados de todo o mundo, rememorando o clássico "1984" de George Orwell[3], agravado na atualidade pela intensa utilização de mecanismos tecnológicos cada vez mais aperfeiçoados.

Escudados em discursos acalorados que invocam a segurança nacional contra o terrorismo, desde 11 de Setembro de 2001 eleito como inimigo comum que deve ser debelado, os Estados Unidos se colocaram à frente de uma verdadeira "cruzada contra o terror", justificando a partir desse argumento inúmeras estratégias claramente invasivas à privacidade. Essas violações aos direitos humanos e fundamentais impõem uma profunda reflexão sobre o assunto, especialmente porque a atuação estadunidense levou inúmeros países a manifestarem repúdio ao vigilantismo, realizado em afronta ao que dispõem inúmeros tratados internacionais e de maneira indiscriminada, como ocorrera.

O sucesso dessas estratégias de espionagem e vigilância é obtido graças ao aperfeiçoamento das Tecnologias da Informação e Comunicação (TIC), que ampliam e aprofundam o *big data* e a *surveillance*, imprimindo ao problema contornos transnacionais. O fato de essas tecnologias, em especial à *Internet*, permitir que a captação de dados seja realizada de maneira velada e além das fronteiras dos Estados, suscita novos problemas que dificilmente serão enfrentados a partir da ação isolada dos países, o que poderia sugerir que instituições como a União Europeia e o próprio Mercado Comum do Sul (Mercosul) poderiam, pela adoção de estratégias harmônicas e articuladas, apresentar melhores condições de enfrentamento do problema. Essa suposição origina o seguinte problema de pesquisa: é possível afirmar que a União Europeia adota medidas de *cibersegurança* que possam fazer frente à atuação dos Estados Unidos? Eventuais medidas, se existentes, encontram correspondente no Mercosul?

[3] "1984", de George Orwell, um clássico da literatura, conta a história de um rapaz, denominado Winston Smith, inconformado com o Estado totalitário que o cerca, representado pelo chamado Grande Irmão. Esse Estado mantém tudo e todos sob constante vigilância, através principalmente das teletelas. No livro, todos aqueles que se revelaram contra o Estado e a sua forma de governo foram severamente punidos (2009). Essa ideia permanece viva na atualidade, agravada pelo aprimoramento das novas tecnologias, pois os seres humanos continuam sendo observados pelos Estados, pelas empresas, especialmente aquelas que armazenam informações e dados pessoais dos usuários de *Internet*, dentre outros. É por essa razão que faz-se primordial a referência à obra.

Para responder a essas indagações parte-se de uma abordagem descendente, na qual analisa-se as estratégias de vigilância realizadas a partir do *big data* e da *surveillance* para demonstrar a violação da privacidade e dos dados de terceiros, passando pela análise específica da *cibersegurança* na União Europeia. Apresentado esse panorama mais geral, na sequência o estudo se volta para o Mercosul, com destaque para o Brasil, que recentemente conta com o Marco Civil da *Internet*, ocasião em que o tratamento normativo conferido à segurança *cibernética* nos dois blocos é contrastado pelo emprego do método comparativo.

1 A ERA DO *BIG DATA* E DA *SURVEILLANCE*: DOS DISCURSOS DECLARADOS EM FAVOR DA SEGURANÇA ÀS ESTRATÉGIAS VELADAS DE VIOLAÇÃO DA PRIVACIDADE.

Vive-se na era do *big data* e da *surveillance*. Para os fins do presente artigo, *big data* significa a capacidade de busca, agregação e referência cruzada de grandes conjuntos de dados, e *surveillance* qualquer sistemática, rotineira e focada atenção aos detalhes pessoais para um determinado propósito (LYON, 2014, p. 2). Esses institutos estão fortemente relacionados com a *ciberespionagem* e a *cibervigilância* em massa que o governo norte-americano realizou e continua realizando, mesmo após as revelações de Edward Snowden em 2013. Antes desse acontecimento, era de conhecimento de poucas pessoas que tudo, ou quase tudo, que fosse compartilhado na *Internet* era passível de monitoramento.

O ano de 2013 destacou-se como o ano em que Edward Snowden revelou ao mundo o maior esquema de espionagem e vigilância *cibernética* da história dos Estados Unidos, comprovado por inúmeros documentos obtidos por ele da *National Security Agency* (*NSA*), a Agência de Segurança Nacional norte-americana (HARDING, 2014).

Snowden é um americano e ex-técnico da *NSA*, que tinha na época dos fatos 29 anos de idade (HARDING, 2014, p. 12). Foi ele quem revelou a Glenn Greenwald e Laura Poitras[4] tudo o que sabia sobre a *surveillance* desempenhada pelo governo dos Estados Unidos. Greenwald escreveu o livro "Sem lugar para se esconder", que narra toda a história do delator, desde os primeiros contatos com o jornalista, até o seu desfecho final, após suas revelações. Nessa ocasião constatou-se que

[4] Glenn Greenwald e Laura Poitras foram os primeiros a entrar em contato com Edward Snowden, foram eles que cobriram as primeiras e mais importantes matérias sobre o caso, através do jornal britânico *The Guardian*, e são eles que possuem todo o acervo de documentos fornecidos pelo delator (HARDING, 2014).

> [...] os arquivos de Snowden expunham de maneira inquestionável uma complexa teia de vigilância de cidadãos tanto americanos (explicitamente fora do escopo da missão da NSA) quanto não americanos. O acervo revelava os recursos técnicos usados para interceptar comunicações: o monitoramento, pela agência, de servidores de internet, satélites, cabos de fibra óptica submarinos, sistemas de telefonia nacionais e estrangeiros e computadores pessoais. Identificava indivíduos escolhidos para serem alvo de formas de espionagem invasivas ao extremo, lista que ia de supostos terroristas e suspeitos de crimes a líderes democraticamente eleitos, de aliados dos Estados Unidos e até mesmo cidadãos norte-americanos comuns. E mostrava quais eram as estratégias e os objetivos gerais da NSA (GLEENWALD, 2014, p. 98-99).

Percebe-se, logo de início, que com o uso da tecnologia o governo norte-americano pôde espionar, vigiar e obter informações e dados de quem quisesse, através principalmente da *Internet* e da telefonia. Harding (2014, p. 14) concluiu que o objetivo final da *NSA* era "coletar tudo, de todos, em todos os lugares, e armazenar por prazo indefinido", o que a faz ignorar por completo o direito à privacidade. Um dos vários programas implementados pela *NSA*, denominado PRISM, permitia à Agência coletar dados diretamente dos serviços das empresas e provedores de *Internet AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo!* e *YouTube*.

Outros programas, como BLARNEY, FAIRVIEW, OAKSTAR e STORMBREW, possibilitavam que a *NSA* interceptasse cabos de fibra óptica de sistemas de telecomunicações e computadores, a fim de coletar informações e dados daqueles que se utilizassem desses recursos (GREENWALD, 2014, p. 108-109). O autor avança nas suas explicações ao afirmar que

> A coleta *upstream* (a partir de cabos de fibra óptica) e a coleta direta nos servidores das empresas de internet (programa PRISM) fornecem a maioria dos registros obtidos pela NSA. Além dessa ampla vigilância, porém, a agência também realiza o que chama de Exploração de Rede Computacional (CNE), inserindo *malwares* em computadores específicos para vigiar seus usuários. Quando consegue inserir *malwares* desse tipo, a NSA torna-se, no jargão da agência, "dona" do computador: passa a ver cada tecla digitada e cada tela visualizada (GREENWALD, 2014, p. 124).

Foi essa vigilância sem precedentes e sem limites, de pessoas físicas, jurídicas e de outros governos, que levou Snowden a delatar todo o esquema de *ciberespionagem* e *cibervigilância* promovido pelos Estados Unidos. Disse ele, ao jornalista Glenn Greenwald (2014, p. 56), "eu não quero viver em um mundo onde não tenhamos privacidade nem liberdade, onde o valor único da internet seja destruído".

Ainda que alguns possam retorquir e criticar a ação do delator, tais práticas não são recentes, encontrando-se relatos de espionagem na Bíblia e no livro "A arte da guerra", escrito

pelo chinês Sunzi, ou Sun Tzu, no século VI a.C.. O fato é que com a emersão das novas tecnologias e com o surgimento do *big data*, a *surveillance*, realizada com o especial auxílio da *Internet*, não só se intensificou como se sofisticou. O *lócus* desse aperfeiçoamento foi os Estados Unidos, país que passou a adotá-la de maneira intensa notadamente após os atentados terroristas de 11 de Setembro de 2001, marco histórico que levou o governo a implementar medidas mais enérgicas em favor da "segurança nacional", violando, em contrapartida, o direito à privacidade e dados pessoais de cidadãos localizados em diversos países[5] (LYON, 2015).

David Lyon (2014, p. 5-10), diretor do *Surveillance Studies Centre* na *Queen's University*, no Canadá, ao analisar a influência do *big data* sob a *surveillance*, expõe três domínios da vigilância, quais sejam: capacidades, consequências e crítica.

Quanto ao domínio das capacidades, o termo *big data* sugere que o tamanho é sua principal característica, e "massive quantities of data about people and their activities are indeed generated by Big Data practices and many corporate and government bodies wish to capitalize on what is understood as the Big Data boom"[6] (LYON, 2014, p. 5). As fontes de dados podem ser obtidas de três formas: a) dirigida: ocorre quando um operador humano obtém os dados; b) automatizada: quando os dados são coletados sem a intervenção de um operador humano, e; c) voluntária: quando os usuários disponibilizam voluntariamente os dados na rede mundial de computadores (LYON, 2014, p. 5).

No que se refere ao domínio das consequências, o autor (LYON, 2014, p. 6) enfatiza três principais formas em que o comprometimento com as práticas de *big data* parecem estar mudando a ênfase da vigilância, quais sejam: 1) automação: a vigilância automatizada tornar-se-á uma possibilidade crescente, principalmente em razão dos algoritmos. Esses são utilizados cada vez mais para atingir tipos específicos de consumidores, contribuindo para o controle *cibernético*. "[...] the price of our freedom in both political and consumer contexts is our shaping or conditioning by algorithms"[7] (LYON, 2014, p. 7); 2) antecipação: as práticas de *big data* inclinam-se cada vez mais para operações de vigilância, focadas mais no futuro, do que no presente ou no passado, e; 3) adaptação: o entusiasmo das "soluções" do *big data* pode levar à

[5] Um estudo denominado "Do NSA's bulk surveillance programs stop terrorists?", divulgado pela *New America Foundation* em 2014, constatou que a *surveillance* da *NSA* não obteve um impacto perceptível quanto à prevenção do terrorismo, pois auxiliou tão somente em 1,8% dos casos dentro dos Estados Unidos e 4,4% dos casos fora daquele país, sendo esses percentuais muito baixos (BERGEN et. al., 2014).

[6] "enormes quantidades de dados sobre pessoas e suas atividades são de fato geradas pelas práticas do Big Data, e muitos organismos empresariais e governamentais desejam capitalizar sobre o que é entendido como o boom do Big Data" (Tradução nossa)

[7] "[...] o preço da nossa liberdade, em ambos os contextos político e de consumo, é a nossa formação ou condicionado por algoritmos" (Tradução nossa)

transferência inapropriada de técnicas de um campo para outro, como, por exemplo, dos provedores de *Internet* para o governo (LYON, 2014, p. 6).

Por fim, quanto ao domínio da crítica, Lyon (2014, p. 9) destaca que "the question of Big Data, understood in relation to the Snowden disclosures, has generated unprecedented public interest in surveillance in many countries around the world"[8]. Contudo, o doutrinador afirma que uma mudança ética torna-se mais urgente como um modo de crítica, observando-se a privacidade, a classificação social e a antecipação. A privacidade é compreendida como um direito humano, isso subjaz aspectos da política democrática, como da liberdade de expressão. Essa ainda é o conceito de mobilização preeminente contra a vigilância inapropriada, desproporcional ou ilegal. O conceito de classificação social alerta para várias práticas relacionadas que produzem resultados irregulares e desiguais, quando as supostamente neutras e iluminadas técnicas de *big data* são aplicadas aos problemas sociais e políticos percebidos. Já a antecipação, diz respeito a como o *big data* promove antecipadamente uma futura abordagem para a vigilância (LYON, 2014, p. 10).

Faz-se importante referir que no atual mundo globalizado, o verdadeiro poder, principalmente para os Estados soberanos, está relacionado com a obtenção de informação[9]. Esses atores passam a exercer o poder não mais em âmbito nacional, pois são ao mesmo tempo locais e globais, adotando a conformação do denominado "Estado em rede" (CASTELLS, 2013, p. 50-51), tema que ganha relevo especialmente em face dos emergentes riscos globais.

Os novos desafios postos aos Estados também são enfrentados por Ulrich Beck (2002, p. 12), conhecido teórico da sociedade global do risco, que sustenta que esse ator está se transformando e perdendo o velho sentido, pois "para realizar o seu "interesse nacional" o Estado da Segunda modernidade deve ativar-se simultaneamente em vários níveis locais e transnacionais e entre instituições muito distantes de suas fronteiras". Conforme sustenta, a democracia, tanto agora quanto no futuro, deve ser reinventada sob um viés transnacional (BECK, 2002, p. 13).

Muito antes desses doutrinadores, Kant (2002, p. 4) propôs um projeto filosófico para a paz perpétua entre os Estados. Dentre os artigos preliminares de sua obra, destaca-se que

[8] "a questão do Big Data, entendido em relação às divulgações de Snowden, tem gerado interesse público sem precedentes na vigilância em muitos países ao redor do mundo" (Tradução nossa)

[9] Para Gilberto Dupas (2001, p. 42) "nas redes, o poder desloca-se para os que detêm o controle dos fluxos". Os Estados Unidos, desde a criação da *Internet*, detêm o poder. Isso significa que, "a sociedade em rede é, por enquanto, uma sociedade capitalista fortemente centrada na dinâmica dos Estados Unidos, que controlam e desenvolvem a maioria das tecnologias envolvidas na dinâmica das redes globais" (DUPAS, 2001, p. 43).

nenhum tratado de paz será considerado válido, se contiver reserva secreta de elementos para uma guerra futura, pois paz pressupõe o fim de todas as hostilidades. Ademais, evidencia-se que nenhum Estado pode impor-se sobre a constituição e o governo de outro Estado, pois isso colocaria em perigo a autonomia de todos os demais (KANT, 2002, p. 7). Para o filósofo, deve ser instaurado um estado de paz, sendo que para tanto, um dos requisitos é a existência de uma federação de Estados livres, que pressupõe um pacto entre os povos para manter a paz de um Estado para si mesmo e a de outros Estados federados, sendo esse um dos artigos definitivos da obra (KANT, 2002, p. 18).

Contudo, parece que a ideia de paz perpétua entre os Estados proposta por Kant está longe de ser concretizada na prática, especialmente em razão do vigilantismo mais acentuado instaurado pelos entes estatais a partir do século XX. A busca incessante por informação e por poder, realizados com o auxílio do *big data* e da *surveillance*, é capaz de originar uma guerra *cibernética* envolvendo os Estados, as empresas públicas e privadas, e a sociedade civil. Saldanha (2013, p. 179), ao fazer alusão ao "Sexto Continente" de Guillebaud, afirma que o mundo *cibernético* é ao mesmo tempo desterritorializado e imediatizado, sendo um solidificador da vigilância global, que além de ser um problema para os Estados-Nação e para a democracia, é também um problema geopolítico difícil de controlar. Nas palavras da autora,

> A cultura da vigilância, no entanto, que institui o "olhar permanente" sobre a sociedade, é o selo da fragilidade da liberdade de expressão e do direito/dever de informação, pois que a destemporalização inverte a sua lógica e contribui para que outros direitos fundamentais sejam violados. Criar antídotos ao controle perfeito é exigência que não compactua com o estado de exceção permanente e assume o compromisso com os avatares da democracia (SALDANHA, 2013, p. 209-210).

Nesse sentido, faz-se importante referir que para Slaughter e White (2006) o futuro do direito internacional é doméstico. Conforme os autores, frente aos novos desafios que o mundo globalizado revela, como o próprio terrorismo, o sistema jurídico internacional tem a função de influenciar na elaboração das leis e na adoção de políticas internas dos Estados, de forma a mobilizar os governos nacionais na persecução de objetivos globais e de metas coletivas. E nem poderia ser diferente, já que o direito à privacidade encontra-se contemplado em Tratados Internacionais, como o Pacto dos Direitos Civil e Políticos[10], internalizado no Brasil pelo

[10] Constam no artigo 17 do Referido Pacto, "1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.".

Decreto Nº 592, de 06 de Julho de 1992, evidenciando o comprometimento dos signatários com o direito à privacidade.

Ocorre que a enunciação de direitos ou a mera previsão normativa interna, por vezes, não se mostram suficientes, sobretudo em face de problemas complexos derivados do uso maciço das TIC. Os limites na atuação isolada dos Estados tanto podem acontecer em razão da carência de governabilidade interna, quanto em virtude de eventual ausência de interesse interno de agir e/ou incapacidade técnica para seu enfrentamento. Partindo dessa constatação, na visão de Slaughter e White (2006), tanto o direito internacional quanto a comunidade internacional estariam legitimados a influenciar, reforçar e dar suporte aos Estados para a elaboração de suas leis e delineamento de políticas internas nacionais.

Marcelo Neves (2009), por sua vez, posiciona-se a favor do transconstitucionalismo e sustenta que problemas constitucionais de direitos fundamentais ou de direitos humanos que ultrapassam as fronteiras dos Estados, exigem a criação de diálogos e conversações transconstitucionais. Para tanto, advoga a necessidade de criar "pontes de transição" entre ordens jurídicas estatais, internacionais, transnacionais, supranacionais e locais, o que deve acontecer em razão da incapacidade dessas ordens em solucionar, isoladamente, os problemas normativos da sociedade mundial. Nesse diapasão, "o método do transconstitucionalismo não pode ter como ponto de partida uma determinada ordem jurídica, muito menos as ordens dos mais poderosos, mas sim os problemas constitucionais que se apresentam enredando as diversas ordens" (NEVES, 2009, p. 275).

O transconstitucionalismo pode ser visto, portanto, como um caminho à proteção das informações e dados de terceiros, pois o direito à privacidade e proteção de dados pessoais é questão de direitos humanos cuja proteção, em tempos de *Internet*, transcende a capacidade das ordens jurídicas locais em barrar e/ou combater a *surveillance*. Ademais, Neves (2009, p. 280-281) também alerta para a infeliz prevalência do código do poder em face do código jurídico, associado à imunização e à intocabilidade de ordens jurídicas como dos Estados Unidos, ou seja, grandes potências perante o direito internacional público.

Mireille Delmas-Marty (2004, p. 194) aponta as condições para a criação de um direito comum a todos, por meio de uma aproximação (e não de uma unificação) dos sistemas e famílias jurídicas. Ao se referir aos direitos do homem, a autora os destaca como o início do processo de transformação, ou seja, recomposição da paisagem jurídica, se aproximando de um direito dos direitos do homem. Assim, "a interação entre direitos não ocorre necessariamente no sentido de uma limitação recíproca. Pode redundar, por uma espécie de efeito de atração,

em reforçar a proteção de um por influência indireta do outro" (DELMAS-MARTY, 2004, p. 192).

Percebe-se que a grande maioria dos autores defende a necessária abertura dos Estados e, por conseguinte, apostam na internacionalização do direito como estratégia para fazer frente aos problemas derivados da sociedade em rede. Diante dos problemas transnacionais da atualidade, como, mais uma vez, o terrorismo, Beck (2002, p. 3) destaca dois modelos de cooperação transnacional entre os Estados, quais sejam os "Estados vigilantes transnacionais" e os "Estados cosmopolitas". O primeiro, embora presente no atual cenário mundial, revela-se um grave problema, pois os Estados transformam-se em "Estados-fortaleza", ou seja, priorizam a segurança e a militarização, com a violação das liberdades e consequente fragilização da democracia. Em contrapartida, no segundo modelo apresentado, os Estados cosmopolitas fundamentam-se no reconhecimento do outro e da alteridade, além de pautarem-se pelo princípio da indiferença nacional do Estado (BECK, 2002, p. 4).

Muito embora existam inúmeros autores que teorizam a respeito do cosmopolitismo e o façam sob perspectivas diversas, faz-se importante citar alguns sem, contudo, exaurir as propostas em face da sua complexidade. O próprio Beck (2011, p. 217) apresenta o "cosmopolitismo real", segundo o qual "o mundo da óptica cosmopolítica é interpretado como uma realidade transparente, no qual as diferenças, as oposições e as fronteiras devem ser olhadas segundo o princípio de que os outros são, na sua essência, idênticos a nós". O autor (2011, p. 222) entende que as relações nacionais/nacionais devem dar lugar as relações translocais, locais/globais, transnacionais, nacionais/globais e globais/globais, denominando-as de "cosmopolitismo metodológico".

Jeremy Waldron (2000, p. 230), por sua vez, discorre sobre o "cosmopolitismo cultural" e o "cosmopolitismo jurídico" de Kant, ratificando a conexão entre ambos. Quanto ao primeiro, o autor destaca:

> […] I think, that the 'essence' of a culture (if indeed that idea makes sense) need not consist in its distinctiveness. One culture does not need to be clearly and importantly *different* from another, either in its appearance to an outsider or in the consciousness of its practitioners, in order to be the culture that it is. A cultural *taxonomist* may be interested in qualitative differentiation, and we as multiculturalists may want there to be lots of colorful differences in costume, language and ritual so that we can *display* our commitment to multiculturalism to even the most superficial glance. […] A culture just is what it is, and its practices and rituals are constitutive of it in virtue of

> their place in a shared way of life, not in virtue of their perceived peculiarity[11] (WALDRON, 2000, p. 233).

Já quanto ao "cosmopolitismo jurídico" de Kant, o doutrinador afirma que esse possui algumas implicações interessantes para as organizações sociais e políticas de determinados Estados territoriais, independentemente dos mais glamorosos negócios do direito internacional, federação de Estados ou comunidades cosmopolitas (WALDRON, 2000, p. 239).

Hauke Brunkhorst (2011, p. 10), por sua vez, apresenta o "cosmopolitismo clássico" como aquele que compreende: 1) ideia de comunidade universal e de única lei básica universal; 2) conjunto de regras procedimentais para solucionar conflitos; 3) direito subjetivo de ouvir e de ser ouvido; 4) leis básicas universais; 5) princípios, métodos e garantias universais, e; 6) princípios universais que não se restrinjam ao direito oficial ou público. Conforme o referido autor (2011, p. 14) "desde a emergência das modernas constituições democráticas no século XVIII, e essa é minha segunda tese, o cosmopolitismo está de volta e, pela primeira vez, é democrático".

Todas as questões abordadas até então possuem uma relação direta com o *big data* e a *surveillance*, violadores do direito à privacidade e proteção de dados pessoais, previstos expressamente no artigo doze da Declaração Universal dos Direitos Humanos de 1948. Portanto, o tratamento do tema exige ações de *cibersegurança* que combinem os âmbitos nacional e transnacional, numa tentativa de ação articulada. Tal constatação impõe que se lance o olhar para o direito derivado da União Europeia, exemplo de organização que conta com recente Diretiva que visa o combate ao vigilantismo, como a seguir demonstrado.

2 A RECENTE DIRETIVA DA UNIÃO EUROPÉIA SOBRE CIBERSEGURANÇA: EXPOSIÇÃO DOS PRINCIPAIS ASPECTOS.

Edward Snowden relatou que, além dos Estados Unidos, alguns países da União Europeia praticaram *surveillance,* não somente nos últimos anos, mas também no passado

[11] [...] Eu acho, que a "essência" de uma cultura (se de fato aquela ideia faz sentido) não precisa consistir em sua distinção. Uma cultura não precisa ser claramente e importantemente diferente de outra, mesmo em sua aparência para um estranho ou na consciência de seus praticantes, a fim de ser a cultura que é. A taxonomista cultural pode estar interessada em diferenciação qualitativa, e nós como multiculturalistas podemos querer que haja muitas diferenças coloridas em trajes, linguagem e ritual para que possamos mostrar o nosso compromisso com o multiculturalismo para nivelar o olhar mais superficial. [...] Uma cultura apenas é o que é, e suas práticas e rituais são constitutivos disso, em virtude de seu lugar de forma compartilhada da vida, não em virtude de suas peculiaridades percebidas. (Tradução nossa)

(GREENWALD, 2014). Trata-se de uma revelação sensível, pois a União Europeia possui trajetória que a identifica pela proteção de direitos de privacidade e de dados pessoais, o que se reflete em textos normativos que datam da década de oitenta[12].

Os acontecimentos dos últimos anos originaram a elaboração de mais um documento, com previsão de entrada em vigor em Agosto de 2016. Trata-se da Diretiva do Parlamento Europeu e do Conselho sobre a segurança das redes e da informação (SRI) em toda a União (CONSELHO EUROPEU, 2016). O caráter inovador do documento e sua oportunidade, posto que vem dar uma resposta às práticas de *surveillance*, justificam o destaque de alguns de seus dispositivos, como se verá na sequência.

Os propósitos e justificativas ficam evidenciados num extenso rol composto por setenta e cinco considerandos que levaram o Parlamento a adotar o documento, destacando-se alguns mais relevantes para os fins do presente estudo. O primeiro refere-se ao reconhecimento da existência de incidentes de segurança, como uma ameaça para o funcionamento das redes e dos sistemas de informação (UNIÃO EUROPEIA, 2016, p. 2). Faz-se importante referir, que a grande maioria dos autores da área da tecnologia, consideram a *Internet* como um ambiente vulnerável a certas ameaças em função da própria arquitetura da rede. No entanto, mesmo assim existem formas pelas quais os profissionais podem dificultar invasões ou a própria *surveillance*, através, por exemplo, da *criptografia*.

A Diretiva aponta a natureza transnacional da rede mundial de computadores e essa configuração aberta faz com que quaisquer perturbações possam afetar tanto a vida e a segurança nos Estados-Membros, quanto a própria estrutura e funcionamento da União Europeia (UNIÃO EUROPEIA, 2016, p. 2). Ao reconhecer formalmente essa configuração verifica-se aproximação com as ideias sustentadas por Castells (2007, p. 245) quanto à

[12] Sobre a proteção de dados pessoais podem ser citados os seguintes documentos produzidos pela União Europeia: a primeira Diretiva que se destaca sobre o tema da proteção dos dados pessoais é a Diretiva 95/46/CE, em 24 de Outubro de 1995, constituindo-se a base sobre a qual novos documentos foram editados. Na sequência foi editada a Diretiva 97/66/CE, de 15 de Dezembro de 1997. Esse documento normatiza o tratamento de dados pessoais e a proteção da privacidade no setor das telecomunicações. Posteriormente editou-se o Regulamento N° 45, de Dezembro de 2000, relativo à proteção dos dados de pessoas singulares recolhidos e tratados por instituições ou órgãos comunitários. Mais especificamente relacionado às comunicações eletrônicas o destaque fica para a Diretiva N° 58, de 2002, denominada de "Diretiva Dados Pessoais nas Comunicações Eletrônicas", ampliada em 2006 em virtude do rápido desenvolvimento tecnológico. A ampliação do escopo desse documento ocorreu pela Diretiva 2006/24/CE, que regulamenta a conservação de dados gerados ou tratados nos serviços de comunicações eletrônicas publicamente disponíveis ou em redes públicas de comunicações. Considerando o rápido avanço das tecnologias e as mais variadas formas de violação, a União Europeia avançou na regulação do tema, editando a Diretiva Nº 136/2009 que inova no campo conceitual na tentativa de precisar com maior clareza o que consistiria a violação de dados pessoais (SILVA; SILVA, 2016).

"sociedade em rede" e a "geografia da Internet" onde se desenham novas configurações fortemente impactadas pelo caráter transnacional.

Ao reconhecer que o problema da *cibersegurança* tanto impacta internamente quanto produz efeitos na própria União, a Diretiva exige que cada Estado integrante desenvolva capacidades e estratégias que garantam um elevado nível de segurança em seus territórios, além de prever a criação de um grupo de cooperação constituído por representantes dos Estados-Membros da União Europeia, cujo trabalho precípuo deve centrar-se na segurança das redes e da informação (ENISA). Esse requisito objetiva promover uma cultura de gestão dos riscos, fundamental para prevenir ataques (UNIÃO EUROPEIA, 2016, p. 3).

As ações articuladas não inibem, no entanto, as medidas referentes aos interesses essenciais da segurança interna de cada Estado, afetas a sua competência e sobre as quais usualmente esses atores se reservam maior margem de autonomia decisória, daí justificando a previsão de que "nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação considere contrária aos interesses essenciais da sua própria segurança" (UNIÃO EUROPEIA, 2016, p. 5).

Por outro lado, cada Estado-Membro deverá implementar uma estratégia nacional de segurança das redes e dos sistemas de informação, definindo objetivos e ações estratégicas concretas a serem executadas (UNIÃO EUROPEIA, 2016, p. 14). Para tanto, é essencial o fortalecimento da cooperação de cada Estado com a União Europeia e da organização para com seus integrantes, o que deve resultar na criação e manutenção de clima de confiança entre todos (UNIÃO EUROPEIA, 2016, p. 15).

No campo das estratégias práticas, fixou-se que cada Estado integrante deve contar com autoridades competentes ou equipes de resposta a incidentes de segurança informática (CSIRT). Considerando o alcance dos incidentes e ataques, a Diretiva em comento destacou a importância da cooperação internacional em matéria de *cibersegurança*, determinando que essas autoridades ou equipes também participem de redes de cooperação internacional (UNIÃO EUROPEIA, 2016, p. 16). Essa previsão reforça o caráter transnacional do tema, que envolve a necessidade de pensar a segurança *cibernética* sob ângulos Estatais, mas também, e principalmente, transnacionais, imposição dada à estrutura aberta da *Internet*.

Nesse documento consta expressamente que, tendo em vista o caráter global dos problemas de segurança que afetam as redes e os sistemas de informação, "é necessário estreitar a cooperação internacional para melhorar as normas de segurança e o intercâmbio de informações e promover uma abordagem comum global das questões de segurança" (UNIÃO

EUROPEIA, 2016, p. 20). Tal previsão só ratifica a ideia de que a segurança da informação e comunicação não será resolvida isoladamente pelos Estados, mas sim mediante a colaboração de todos os entes estatais e não estatais, o que implica no estabelecimento de relação de solidariedade entre todos os atores envolvidos.

O caráter multisetorial também se faz evidente, já que o referido documento prevê deveres também aos prestadores de serviços digitais, incluindo os provedores de *Internet*. Para esses estabelece-se a obrigação de garantir um certo nível de segurança que seja proporcional aos riscos que fornecem. Os fabricantes de *hardware* e os desenvolvedores de *software* igualmente são mencionados, recaindo sobre eles o dever de fazer com que os seus produtos reforcem a segurança das redes e dos sistemas (UNIÃO EUROPEIA, 2016, p. 22).

E a preocupação não é somente com os dados governamentais ou da União Europeia, pois a Diretiva também contempla os incidentes com dados pessoais de terceiros. Nesse caso, as autoridades responsáveis devem cooperar e trocar informações que possam prevenir ou, na sua impossibilidade, combater tais violações (UNIÃO EUROPEIA, 2016, p. 26).

Os limites da atuação isolada dos Estados nacionais ficam plasmados em passagem expressa no final da primeira parte dessa Diretiva, onde expressamente seus signatários reconhecem que "atingir um elevado nível comum de segurança das redes e dos sistemas de informação na União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação considerada, ser mais bem alcançado ao nível da União" (UNIÃO EUROPEIA, 2016, p. 31).

Após esses considerandos iniciais, são apresentados os artigos da Diretiva que visam dar condições de cumprimento dos propósitos firmados, não cabendo, nos reduzidos limites desse trabalho, abordar individualmente cada um. Sobressai, em linhas gerais, no entanto, o reconhecimento formal de que a *surveillance*, por dizer respeito à segurança das informações e dados de terceiros na rede mundial de computadores, é melhor combatida em conjunto, pelos Estados, cujas ações individuais não são suficientes para fazer frente a problemas globais.

3 A POSTURA MERCOSULINA NO COMBATE À *SURVEILLANCE* E A POSIÇÃO DO BRASIL A PARTIR DA LEI Nº 12.965/2014.

As revelações feitas pelo ex-técnico da *NSA* evidenciaram que as técnicas e estratégias de *cibervigilância* e *ciberespionagem* empreendidas pelos Estados Unidos também ocorriam

desse lado do Atlântico, e atingiam fluxos informacionais originados ou transmitidos pelos Estados e cidadãos pertencentes ao Mercado Comum do Sul.

Tal situação levou a um pronunciamento dos representantes desse bloco, reprovando o vigilantismo norte-americano. A BBC (2013) noticiou que "Mercosul rechaça espionagem e deixa em aberto asilo a Snowden" e "Mercosul reforça na ONU 'indignação' com espionagem dos EUA". Ainda no ano de 2013, foi divulgado pela mídia a intenção do Mercosul em criar um grupo permanente contra a *surveillance*, contudo, esse projeto não se desenvolveu, pois até o ano de 2016 não foi implementado (TADDEO, 2013), o que demonstra sua timidez e incapacidade de articulação política se comparado àquela demonstrada pela União Europeia.

Sabe-se das diferenças existentes entre o Mercosul e a União Europeia[13], marcadas não somente pelo seu histórico de criação e pelo seu tempo de existência, como também pela condição econômica e social dos Estados latinos, nitidamente menos desenvolvidos em comparação com os integrantes do bloco europeu.

Ademais, enquanto a União Europeia é supranacional e adepta do direito comunitário, onde há a primazia desse em relação às normas nacionais, o Mercosul mantém estrutura intergovernamental e é adepto do direito da integração. Essa distinção faz com que Machado e Del'Olmo (2011, p. 218) afirmem que "a principal característica do Direito da União consiste na possibilidade de aplicação imediata e de produção direta de efeitos no território dos Estados membros", já "no MERCOSUL as fontes do Direito da Integração não possuem aplicabilidade imediata e efeito direito. A incorporação das normas obedece ao processo tradicional de celebração dos tratados internacionais. O que se adota é a teoria do efeito indireto".

Como é possível perceber, o Mercosul e a União Europeia possuem características distintas, contudo, nada impede que o Mercosul, assim como fez a União Europeia, atue para proteger seus Estados-Membros das práticas de *surveillance*, pois como já referido anteriormente, os países em conjunto possuem capacidade de atuação maior àquela demonstrada isoladamente.

[13] Esta surgiu com o Tratado de Paris, em 1951, e tornou-se união econômica e monetária com o Tratado da União Europeia (ou Tratado de Maastricht), em 1993. Já o Mercosul teve início com o Tratado de Assunção, em 1991, e constitui-se em união aduaneira incompleta. Enquanto as principais fontes secundárias da União Europeia são regulamentos, diretivas, decisões, recomendações e pareceres, as do Mercosul são decisões, resoluções e diretrizes (MACHADO; DEL'OLMO, 2011, p. 217).

A insuficiência da atuação isolada ficou muito clara no caso brasileiro, também alvo do vigilantismo estadunidense e que respondeu a essas práticas com a promulgação da Lei Nº 12.965/2014, nominada de Marco Civil da *Internet*.

Ainda que sua edição tenha apressado o processo regular de sua produção colaborativa e essa lei tenha sido anunciada como uma resposta brasileira à delação de Snowden, na verdade ela não trata especificamente do tema, inexistindo no país uma norma específica que vise barrar e/ou combater a *surveillance*.

Os autores não negam a importância da norma, e inclusive citam-no como uma lei modelo para os demais Estados. Antes de 2014 o país não contava com uma legislação regulamentadora da *Internet*, por isso o Marco Civil se mostra uma norma de grande relevo. Contudo, existem críticas quanto ao seu texto, especialmente por não aprofundar questões atinentes à proteção de dados pessoais e, além disso, não abranger a *cibersegurança* como uma estratégia às revelações de Edward Snowden em 2013.

Morais e Menezes Neto (2014, p. 15) corroboram esse entendimento e afirmam que o Marco Civil fracassou, pois "seria ingênuo – embora essa espécie de pensamento seja extremamente comum no imaginário jurídico – acreditar que esse tipo de solução sólida (dispositivo legal) tem condições para lidar com a liquidez da *surveillance*". De fato, a mera previsão normativa não é capaz, isoladamente, de resolver o problema da vigilância cibernética, que além de exigir estratégias políticas, envolve outras áreas do conhecimento, como a própria tecnologia.

Inúmeros autores, como Meyer-Pflug e Leite (2015, p. 444), assim como Barbosa (2015, p. 249), desenvolveram estudos e concluíram pela insuficiência legislativa no combate ao vigilantismo no Brasil, e alguns sustentam uma solução em âmbito internacional. Essa solução, que transcende as fronteiras dos Estados, pode ter como ponto de partida, ou até mesmo como modelo a ser adotado, a Diretiva da União Europeia sobre *cibersegurança*, exposta na segunda seção deste trabalho.

Isso porque, conforme Silva (2014, p. 93), os Estados devem cooperar uns com os outros no combate a tais práticas. A autora inclusive sugere a implantação de Centros Nacionais de *Cibersegurança* pelos Estados, para auxiliar nessa tarefa. Deve-se ter em mente que os problemas que surgem a partir do *big data* e da *surveillance*, como a violação da privacidade e dados pessoais, afetam toda a sociedade (SILVA, 2014, p. 90). É nesse mesmo sentido que Pilati e Olivo (2014, p. 293) analisam o direito à privacidade como um bem coletivo, e não mais individual, pois no contexto da sociedade em rede os problemas (nesse caso de privacidade e

proteção de dados de terceiros) são transferidos para o âmbito da sociedade, como sujeito de direitos coletivos.

Percebe-se, portanto, que as questões que atualmente impactam o direito à privacidade e proteção de dados pessoais ultrapassam a mera visão individualista de outrora e ganham novos contornos, coletivos e de interesse internacional, o que remete o tema à seara dos direitos humanos. E nesse sentido, vale lembrar que a Declaração Universal dos Direitos Humanos de 1948, já citada anteriormente, "objetiva delinear uma ordem pública mundial fundada no respeito à dignidade humana, ao consagrar valores básicos universais" (PIOVESAN, 2015, p. 216). O princípio da dignidade da pessoa humana é regra norteadora dos direitos humanos e fundamentais, pois é a partir desse princípio que se impõe um mínimo ético a ser observado por todos os atores que se movem no cenário internacional, como sustentado por Flávia Piovesan (2015, p. 235).

O reconhecimento dos novos contornos do direito à privacidade, que a um só tempo envolve interesse individual e coletivo, nacional e internacional, exige novo tratamento do tema. Nesse sentido, pode-se destacar a atuação brasileira com a recente edição do Decreto Nº 8.793/2016, de Junho de 2016. Esse documento fixa a Política Nacional de Inteligência e parte do conceito de espionagem como "a ação que visa à obtenção de conhecimentos ou dados sensíveis para beneficiar Estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos". Também prevê, como uma diretriz, prevenir ações de espionagem no país (BRASIL, 2016).

Nesse documento, o combate à espionagem e vigilância é referido como a prioridade principal, isso porque parte do entendimento de que "ações de espionagem podem afetar o desenvolvimento socioeconômico e comprometer a soberania nacional. Há instituições e empresas brasileiras vulneráveis à espionagem, notadamente aquelas que atuam nas áreas econômico-financeira e científico-tecnológica" (BRASIL, 2016). Ademais, o documento reconhece que "a conjuntura mundial tem alterado a percepção e a conduta dos Estados nacionais, das organizações e dos indivíduos, realçando os chamados temas globais e transnacionais", aduzindo que "a complexidade global já não permite clara diferenciação de aspectos internos e externos na identificação da origem das ameaças e aponta, cada vez mais, para a necessidade de que sejam entendidas, analisadas e avaliadas de forma integrada" (BRASIL, 2016).

Assim, ao delinear as políticas de inteligência internas, o Brasil reconhece claramente a necessidade de que o tratamento das questões internas de inteligência e segurança de dados

ocorra em proteção ao Estado e à sociedade brasileira, mas sem ignorar a política externa do país, já que esse tema possui clara interface internacional, como destacado pelo próprio documento.

Considerando esse reconhecimento expresso, nada impede que junto a essas medidas de inteligência previstas para o Brasil também sejam adotadas ações no âmbito do Mercosul, visando à proteção de informações e dados pessoais e dos órgãos públicos. Tal medida não se chocaria com a política interna, já que poderia complementá-la, pois Argentina e Uruguai podem aportar grandes contribuições, especialmente em razão de contarem com legislações específicas de proteção de dados pessoais, com o mesmo nível de adequação existente na União Europeia.

CONCLUSÃO

Frente ao exposto neste trabalho, conclui-se que de fato as revelações de Edward Snowden em 2013 modificaram o cenário internacional. A comprovação das práticas de *surveillance* pelos Estados Unidos aumentou as preocupações de inúmeros países quanto à proteção da privacidade e dados de terceiros, posto que nem mesmo os governos escaparam àquele vigilantismo.

Ainda que as justificativas para essas práticas sejam o combate ao terrorismo, sabe-se que as estratégias de *big data* associadas à *surveillance* não respondem eficazmente para a proteção da segurança nacional ou internacional, posto que após os atentados terroristas de 11 de Setembro de 2001, muitos outros ataques aconteceram sem que o governo norte-americano conseguisse evitar.

Na tentativa de enfrentar esse problema global, recentemente a União Europeia adotou uma Diretiva sobre *cibersegurança*. Destaca-se, no texto, um claro direcionamento para a colaboração dos Estados-Membros para com a União Europeia e vice versa, em relação à segurança *cibernética*. Essa medida é vista como positiva, pois se entende que temas complexos e transversais como esse, exigem diálogos e conversações através das pontes de transição, teorizadas por Marcelo Neves, que têm potencial para prevenir e amenizar os efeitos do vigilantismo dos Estados Unidos.

Ao contrário das providências adotadas na União Europeia, no Mercosul não se registram medidas de ação conjunta no intuito de promover a *cibersegurança* dos países do

bloco, e ainda que os Estados integrantes tenham repudiado as práticas norte-americanas, nenhum documento foi editado em resposta a elas.

O Brasil, por sua vez, não conta com lei específica sobre proteção de dados pessoais, contudo o Marco Civil da *Internet* aborda algumas questões sobre privacidade, ao que se pode reunir o recente Decreto que estabelece as ações de inteligência. Mesmo assim, conforme os doutrinadores, a legislação nacional não é capaz de barrar e/ou combater a *ciberespionagem* e a *cibervigilância*, cujo enfrentamento exige ações conjuntas, reunindo esforços nacionais e internacionais.

Sustenta-se que esse tema deve ser incluído na pauta de discussão no âmbito do Mercosul, pois ainda que algumas questões sejam de interesse eminentemente nacional, a fluidez das informações e dados pessoais ultrapassam as fronteiras dos Estados e exigem articulação e colaboração desses. Nesse sentido, a experiência argentina e uruguaia, que já contam com leis específicas de proteção de dados pessoais, poderia ser muito rica para o estabelecimento de políticas e ações coordenadas dentro do bloco, as quais teriam melhores condições de enfrentamento de temas transversais e transnacionais como esse.

REFERÊNCIAS

BARBOSA, Marco A.. Marco civil da internet: mercado e estado de vigilância. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo II:** Marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

BECK, Ulrich. O Estado cosmopolita: para uma utopia realista. **Eurozine.** Tradução de Adriana Bebiano. 30 jan. 2002. Disponível em: <http://www.eurozine.com/articles/2002-01-30-beck-pt.html>. Acesso em: 13 jun. 2016.

_____. Qu'est le cosmopolitisme? Tradução de Lurdes Macedo. **Caleidoscópio – Revista de Comunicação e Cultura.** n. 10, 2011. Disponível em: <http://revistas.ulusofona.pt/index.php/caleidoscopio/article/view/3719/2499>. Acesso em: 13 jun. 2016.

BERGEN, Peter; STERMAN, David; SCHNEIDER, Emily; CAHALL, Bailey. Do NSA's bulk surveillance programs stop terrorists? **New America Foundation**, 2014. Disponível em: <https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/>. Acesso em: 06 jun. 2016.

BRASIL. **Decreto nº 592, de 06 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>. Acesso em: 19 set. 2016.

_____. **Decreto n. 8.793, de 29 de junho de 2016.** Fixa a política nacional de inteligência; Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8793.htm>. Acesso em: 15 jul. 2016.

_____. **Marco Civil da Internet.** Lei n. 12.965, de 23 de abril de 2014. Publicada no Diário Oficial da União, de 24-4-2014. Vade Mecum OAB e concursos. 8. ed. São Paulo: Saraiva, 2016.

BRUNKHORST, Hauke. Alguns problemas conceituais e estruturais do cosmopolitismo global. Tradução de Sebastião Nascimento. **RBCS**, vol. 26, n. 76, jun./2011. Disponível em: <http://www.scielo.br/pdf/rbcsoc/v26n76/02.pdf>. Acesso em: 13 jun. 2016.

CASTELLS, Manuel. **A galáxia internet:** reflexões sobre internet, negócios e sociedade. Tradução de Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2007.

_____. **O poder da comunicação.** Tradução de Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2013.

CONSELHO EUROPEU. Conselho da União Europeia. **Conselho aprova regras em matéria de cibersegurança a nível da UE.** 17 mai. 2016. Disponível em: <http://www.consilium.europa.eu/pt/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/>. Acesso em: 15 jun. 2016.

DELMAS-MARTY, Mireille. **Por um direito comum.** Tradução Maria Ermantina de Almeida Prado Galvão. São Paulo: Martins Fontes, 2004.

DUPAS, Gilberto. **Ética e poder na sociedade da informação:** de como a autonomia das novas tecnologias obriga a rever o mito do progresso. São Paulo: Editora UNESP, 2001.

GREENWALD, Glenn. **Sem lugar para se esconder.** Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

HARDING, Luke. **Os arquivos Snowden:** a história secreta do homem mais procurado do mundo. Tradução de Alice Klesck e Bruno Correia. Rio de Janeiro: LeYa, 2014.

KANT, Immanuel. **A paz perpétua:** um projeto filosófico. Tradutor Artur Morão. Covilhã: LusoSofia.press, 2008. Disponível em: <http://www.lusosofia.net/textos/kant_immanuel_paz_perpetua.pdf>. Acesso em: 07 jun. 2016.

LYON, David. **Surveillance after Snowden.** Cambridge, UK: Polity Press, 2015.

_____. Surveillance, Snowden, and big data: capacities, consequences, critique. **Big Data & Society.** July-December 2014: 1-13. Disponível em: <http://bds.sagepub.com/content/1/2/2053951714541861>. Acesso em: 05 jun. 2016.

MACHADO, Diego Pereira; DEL'OLMO, Florisbal de Souza. **Direito da integração, direito comunitário, Mercosul e União Europeia.** Salvador – Bahia: JusPODIVM, 2011.

MEYER-PFLUG, Samantha Ribeiro; LEITE, Flavia Piva Almeida. A liberdade de expressão e o direito à privacidade no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo I:** marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

MORAIS, Jose Luis Bolzan; MENEZES NETO, Elias Jacob de. Surveillance e estado-nação: as inadequadas tentativas de controlar os fluxos de dados através do marco civil da

internet e da CPI da espionagem. In: XXIII Congresso Nacional do CONPEDI, 2014, João Pessoa – Paraíba. **Anais Direito e Novas Tecnologias I.** Disponível em: <http://publicadireito.com.br/artigos/?cod=2f7eaf16eceec07f>. Acesso em: 20 jun. 2016.

MOTA, Denise. Mercosul rechaça espionagem e deixa em aberto asilo a Snowden. **BBC Brasil**, jul. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/07/130712_mercosul_reuniao_snowden_dm_lgb>. Acesso em: 25 jun. 2016.

NEVES, Marcelo. **Transconstitucionalismo.** São Paulo: Editora WMF Martins Fontes, 2009.

ORWELL, George. **1984.** Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PILATI, José Isaac; OLIVO, Mikhail Vieira Cancelier de. Um novo olhar sobre o direito à privacidade: caso Snowden e pós-modernidade jurídica. **Seqüência:** Estudos Jurídicos e Políticos. Florianópolis, v. 35, n. 69, p. 281-300, dez. 2014. ISSN 2177-7055. Disponível em: < https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2014v35n69p281/28392>. Acesso em: 21 jun. 2016.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional.** 15.ed. São Paulo: Saraiva, 2015.

SALDANHA, Jânia Maria Lopes. Os desafíos do "império cibernético" na era da aceleração e da informação: um "sexto continente" de liberdade perfeita ou de controle perfeito? In: TYBUSCH, Jerônimo Siqueira; ARAUJO, Luiz Ernani Bonesso de; SILVA, Rosane Leal da. **Direitos emergentes na sociedade global:** anuário do programa de pós-graduação em direito da UFSM. Ijuí: Ed. Unijuí, 2013.

SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto português.** 2014. 112p. Dissertação (Mestrado em Guerra da Informação), Academia Militar, Lisboa, Portugal, 2014. Disponível em:

<http://comum.rcaap.pt/bitstream/123456789/8750/1/Ciberespionagem%20no%20Contexto%20Portugu%C3%AAs%20Jul%202014%20Susana%20Silva.pdf>. Acesso em: 20 jun. 2016.

SILVA, Letícia Brum da; SILVA, Rosane Leal da. **A proteção jurídica de dados pessoais na internet**: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>. Acesso em: 19 set. 2016.

SLAUGHTER, Anne-Marie; WHITE, William Burke. The future of international law is domestic (or, the European way of law). **Harvard International Law Journal**, vol. 47, n. 2, summer 2006. Disponível em: <http://www.harvardilj.org/wp-content/uploads/2010/09/HILJ_47-2_Slaughter_Burke-White.pdf>. Acesso em: 08 jun. 2016.

SUNZI. **A arte da guerra.** Tradução e edição Adam Sun. São Paulo: Conrad Editora do Brasil, 2006.

TADDEO, Luciana. Mercosul terá grupo permanente contra espionagem. **Operamundi**, out. 2013. Disponível em: <http://operamundi.uol.com.br/conteudo/noticias/32157/mercosul+tera+grupo+permanente+contra+espionagem.shtml>. Acesso em: 25 jun. 2016.

UCHOA, Pablo. Mercosul reforça na ONU 'indignação' com espionagem dos EUA. **BBC Brasil**, ago. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/08/130730_patriota_eua_mdb_pu>. Acesso em: 25 jun. 2016.

UNIÃO EUROPEIA. **Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.** 2016. Disponível em: <http://data.consilium.europa.eu/doc/document/ST-5581-2016-INIT/pt/pdf>. Acesso em: 15 jun. 2016.

WALDRON, Jeremy. What is cosmopolitan? **The Journal of Political Philosophy:** volume 8, n. 2, 2000, pp. 227-243. Disponível em: <http://detc.ls.urfu.ru/courses/cphilos0021/text/hrest_03_03_07.pdf>. Acesso em: 13 jun. 2016.

ZOLO, Danilo; BECK, Ulrich. A sociedade global do risco: um diálogo entre Danilo Zolo e Ulrich Beck. **Prim@ Facie International Journal.** Ano 1, n. 1, jul./dez. 2002. Disponível em: <http://periodicos.ufpb.br/ojs/index.php/primafacie/article/view/4245/3195>. Acesso em: 06 jun. 2016.